PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-186546
(43)Date of publication of application : 16.07.1996

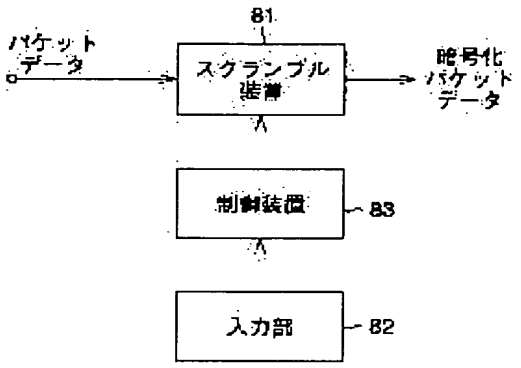
(51)Int.Cl. H04H 1/00
G09C 1/00
H04L 9/18
H04N 7/167

(21)Application number : 06-328027
(22)Date of filing : 28.12.1994

(71)Applicant : SONY CORP
(72)Inventor : YAMASHITA MASAMI

(54) SYSTEM AND METHOD FOR SCRAMBLE AND SYSTEM AND METHOD FOR DESCRAMBLE

(57)Abstract:
PURPOSE: To provide information in a state rich in changes.
CONSTITUTION: A control circuit 83 controls a scrambler 81 corresponding to an input from an input part 82 and scrambles video data or audio data for the unit of a packet. In a first mode, only the video data are scrambled, in a second mode, only the audio data are scrambled, in a third mode, both the video data and audio data are scrambled and in a fourth mode, the video data and the audio data are respectively alternately scrambled.



LEGAL STATUS

[Date of request for examination]	05.07.2001
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	abandonment
[Date of final disposal for application]	25.01.2005
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

THIS PAGE BLANK (USPTO)

THIS PAGE BLANK (USPTO)

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－186546

(43)公開日　平成８年(1996)７月16日

(51)Int.Cl.[6]	識別記号	ＦＩ
H04H 1/00	F	
	H	
G09C 1/00	7259-5J	
		H04L 9/02　B
		H04N 7/167

審査請求　未請求　請求項の数６　ＯＬ　（全13頁）　最終頁に続く

(21)出願番号　特願平6－328027

(22)出願日　平成６年(1994)12月28日

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　山下　雅美
東京都品川区北品川６丁目７番35号　ソニー株式会社内

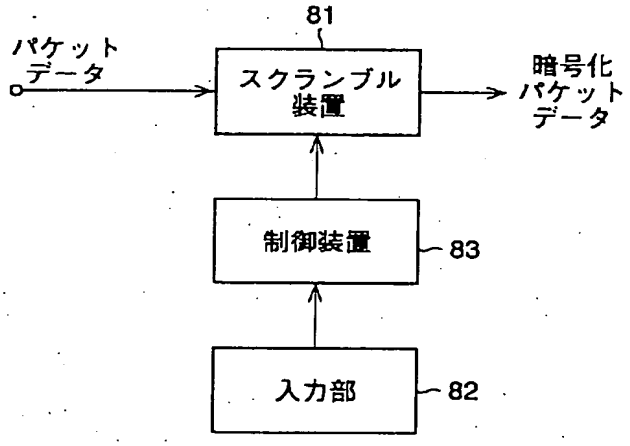
(74)代理人　弁理士　稲本　義雄

(54)【発明の名称】スクランブルシステムおよび方法並びにデスクランブルシステムおよび方法

(57)【要約】

【目的】　変化に富んだ状態で情報を提供できるようにする。

【構成】　入力部８２からの入力に対応して制御回路８３はスクランブル装置８１を制御し、パケット単位でビデオデータまたはオーディオデータをスクランブルする。第１のモードのときビデオデータだけを、第２のモードのときオーディオデータだけを、第３のモードのときビデオデータとオーディオデータの両方を、第４のモードのときビデオデータとオーディオデータを交互に、それぞれスクランブルする。



1

【特許請求の範囲】

【請求項１】　パケットを単位として伝送するビデオデータとオーディオデータの少なくとも一方を、前記パケットを単位としてスクランブルするスクランブル装置において、

前記パケットに含まれるデータが、前記ビデオデータまたはオーディオデータであることを表すＩＤを検出する検出手段と、

前記ビデオデータをスクランブルする第１のモード、前記オーディオデータをスクランブルする第２のモード、前記ビデオデータとオーディオデータの両方を同時にスクランブルする第３のモード、前記ビデオデータとオーディオデータを選択的にスクランブルする第４のモードのうちの少なくとも２つのモードの１つを選択的に設定する設定手段と、

類似ランダム系列を発生する発生手段と、

前記発生手段の出力する前記類似ランダム系列を前記ビデオデータまたはオーディオイデータに加算する加算手段と、

前記設定手段により設定された前記モードと、前記検出手段により検出された前記ＩＤに対応して、前記類似ランダム系列の前記加算手段への供給を制御する制御手段とを備えることを特徴とするスクランブルシステム。

【請求項２】　前記類似ランダム系列を生成するための初期値を、前記検出手段により検出された前記ＩＤに対応して修整する修整手段をさらに備えることを特徴とする請求項１に記載のスクランブルシステム。

【請求項３】　パケットを単位として伝送されるとともに、前記パケットを単位としてスクランブルされているビデオデータとオーディオデータの少なくとも一方をデスクランブルするデスクランブル装置において、

前記パケットに含まれるデータが、前記ビデオデータまたはオーディオデータであることを表すＩＤを検出する検出手段と、

前記ビデオデータをデスクランブルする第１のモード、前記オーディオデータをデスクランブルする第２のモード、前記ビデオデータとオーディオデータの両方を同時にデスクランブルする第３のモード、前記ビデオデータとオーディオデータを選択的にデスクランブルする第４のモードのうちの少なくとも２つのモードの１つを選択的に設定する設定手段と、

類似ランダム系列を発生する発生手段と、

前記発生手段の出力する前記類似ランダム系列を前記ビデオデータまたはオーディオイデータに加算する加算手段と、

前記設定手段より設定された前記モードと、前記検出手段により検出された前記ＩＤに対応して、前記類似ランダム系列の前記加算手段への供給を制御する制御手段とを備えることを特徴とするデスクランブルシステム。

【請求項４】　前記類似ランダム系列を生成するための初期値を、前記検出手段により検出された前記ＩＤに対応して修整する修整手段をさらに備えることを特徴とする請求項３に記載のデスクランブルシステム。

【請求項５】　パケットを単位として伝送するビデオデータとオーディオデータの少なくとも一方を、前記パケットを単位としてスクランブルするスクランブル方法において、

前記パケットに含まれるデータが、前記ビデオデータまたはオーディオデータであることを表すＩＤを検出し、

前記ビデオデータをスクランブルする第１のモード、前記オーディオデータをスクランブルする第２のモード、前記ビデオデータとオーディオデータの両方を同時にスクランブルする第３のモード、前記ビデオデータとオーディオデータを選択的にスクランブルする第４のモードのうちの少なくとも２つのモードの１つを選択的に設定し、

類似ランダム系列を発生し、

前記発生手段の出力する前記類似ランダム系列を前記ビデオデータまたはオーディオイデータに加算し、

設定された前記モードと、検出された前記ＩＤに対応して、前記類似ランダム系列の前記加算手段への供給を制御することを特徴とするスクランブル方法。

【請求項６】　パケットを単位として伝送されるとともに、前記パケットを単位としてスクランブルされているビデオデータとオーディオデータの少なくとも一方をデスクランブルするデスクランブル方法において、

前記パケットに含まれるデータが、前記ビデオデータまたはオーディオデータであることを表すＩＤを検出し、

前記ビデオデータをデスクランブルする第１のモード、前記オーディオデータをデスクランブルする第２のモード、前記ビデオデータとオーディオデータの両方を同時にデスクランブルする第３のモード、前記ビデオデータとオーディオデータを選択的にデスクランブルする第４のモードのうちの少なくとも２つのモードの１つを選択的に設定し、

類似ランダム系列を発生し、

前記類似ランダム系列を前記ビデオデータまたはオーディオイデータに加算し、

設定された前記モードと、検出された前記ＩＤに対応して、前記類似ランダム系列の前記ビデオデータまたはオーディオイデータへの加算を制御することを特徴とするデスクランブル方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、例えば映像、音声などのデジタルデータを放送衛星、通信衛星などを介して伝送するデジタル放送システムにおいて、デジタルデータをスクランブルまたはデスクランブルする場合に用いて好適なスクランブルシステムおよび方法、並びにデスクランブルシステムおよび方法に関する。

2

【０００２】

【従来の技術】契約放送においては、スクランブル放送と呼ばれる放送方式が用いられることが多い。このスクランブル放送は、放送局側において、元信号を所定の方法で意図的に乱すことにより、放送局と契約していない者が放送を受信しても、正常な画像や音声データなどを利用することが出来ないようにするものである。放送局と契約した者に対しては、デコーダを与え、このデコーダによりスクランブルされているデータを元の形にデスクランブルすることで、正常な画像、音声データなどを得ることが出来るようにする。

【０００３】スクランブル放送においては、契約をしていない者に放送が受信された場合においても、その内容を知られないようにするために、出来るだけデスクランブルすることが困難な方法でスクランブルすることが望ましい。

【０００４】スクランブルの方式は、大きく２つに分類される。１つはストリームサイファであり、他の１つはブロックサイファである。

【０００５】ストリームサイファは、疑似ランダム信号を発生させ、この疑似ランダム信号を元信号にモジュロ２加算することにより、元信号をスクランブルする方法である。

【０００６】これに対してブロックサイファは、ＤＥＳ（Ｄａｔａ　ＥｎｃｒｙｐｔｉｏｎＳｔａｎｄａｒｄ）のように、ブロック単位で元信号を区切り、各ブロックで複雑な処理を繰り返す方法である。

【０００７】ストリームサイファは、ハードウエア構成が簡単である利点を有する反面、解読されやすいという欠点を有している。これに対してブロックサイファは、解読されにくいという利点を有する反面、ハードウエア構成が複雑になるという欠点を有している。

【０００８】ＩＳＯ（Ｉｎｔｅｒｎａｔｉｏｎａｌ　Ｏｒｇａｎｉｚａｔｉｏｎ　ｆｏｒＳｔａｎｄａｒｄｉｚａｔｉｏｎ）／ＩＥＣ（Ｉｎｔｅｒｎａｔｉｏｎａｌ　Ｅｌｅｃｔｏｒｏ－ｔｅｃｈｎｊｃａｌ　Ｃｏｍｉｓｓｉｏｎ）１３８１８－１（ＭＰＥＧ２　Ｓｙｓｔｅｍｓ）では、トランスポートパケットを単位として、マルチメディアのデータを多重化して伝送することが標準化されている。このパケットは１８８バイトの長さを有しており、デジタル映像、デジタル音声、データ信号が、パケット単位で多重化されている。多重化を柔軟に行うためには、パケット単位でスクランブルが完結するようにした方が、以後の伝送系においてパケットの編集などを自由に行うことができるため好ましい。またその方が、パケットの脱落などに関しても影響が少ない。

【０００９】ところで放送衛星を介して伝送するデータをスクランブルする装置として、平成５年６月２１日の「電気通信技術審議会答申」により、「諮問第５３号「放送衛星によるデータ放送に関する技術的条件」のうち、伝送制御方式および有料方式ならびにファクシミリ、テレソフトウエア、静止画、文字（基本）、時刻の各信号の技術的条件」として、図７に示すスクランブル装置が提案されている。

【００１０】スクランブルキーは、３２ビットの初期値と、４ビットの修整制御値よりなり、初期値を初期値レジスタ１にロードされ、修整制御値は修整制御レジスタ５にロードされる。このロードはキー更新タイミングフラグＳＣＴが１のパケットのとき行われる。

【００１１】初期値レジスタ１は、３２段のフィードバックシフトレジスタにより構成されている。この初期値レジスタ１にロードされたデータは、下位ビットから上位ビットへシフト信号に対応してシフトが行われる。

【００１２】前のパケットの連続性指標ＣＩの値（０乃至１５のいずれかの値をとる）が１５で、当該パケットのＣＩの値が０であるとき、ＣＩのキャリーが１とされる。ＣＩのキャリーはそのほかの場合（連続性指標が１５のパケットから０のパケットへの変化以外の変化である場合）、０となっている。このＣＩの値が１で、修整制御レジスタ５の出力ｆ３が１のとき、アンドゲート１０が論理１を出力する。この論理１が、スクランブルキー更新タイミングフラグＳＣＴが０であるとき、すなわち初期値レジスタ１にロードが行われる以外のとき、アンドゲート６を介して、シフト信号として初期値レジスタ１に入力される。初期値レジスタ１は、この論理１のシフト信号に対応してシフト動作を行う。

【００１３】初期値レジスタ１より出力された３２ビットの初期値は、初期値修整回路２に入力され、修整される。この修整は、修整制御レジスタ５の出力ｆ０乃至ｆ２と、デジタルデータを伝送する論理チャンネルを識別するための論理チャンネル識別ＬＣＩ１，ＬＣＩ２および連続性指標ＣＩをアンドゲート７乃至９で論理積して得た初期値修整データに対応して行われる。

【００１４】初期値修整回路２が出力する修整された初期値は、ＰＲＰＳ（Ｐｓｅｕｄｏ－ｒａｎｄｏｍ　ｂｉｎａｒｙ　ｓｅｑｕｅｎｃｅ：疑似ランダム２値信号系列）、生成回路３に入力される。ＰＲＢＳ生成回路３は所定のロード信号が入力されたとき、この修整された初期値をロードし、アンドゲート１１を介して所定のシフト信号が入力されたとき、その修整された初期値をシフトして、ＰＮ信号（疑似ランダム信号）を生成する。このＰＮ信号はスクランブル識別フラグＳＣＦが１のとき、アンドゲート４を通過し、加算器１２に入力される。加算器１２はアンドゲート４から入力されたＰＮ信号を、図示せぬ回路から供給されたパケットデータに加算し、暗号化されたパケットデータとして出力する。

【００１５】この装置を、上述したＭＰＥＧ２　Ｓｙｓｔｅｍｓのトランスポートパケットのスクランブルに用いることが考えられる。

【００１６】

5

【発明が解決しようとする課題】しかしながら、従来のスクランブル装置においては、例えば、所定の番組のデータをスクランブルする場合、そのビデオデータをスクランブルするだけでなく、オーディオデータもスクランブルするようになされており、ビデオデータだけ、あるいはオーディオデータだけを独立にスクランブルすることができない課題があった。その結果、提供できる情報の状態が画一的となり、提供する情報に対応して、変化に富んだ状態で情報を提供することができない課題があった。

【００１７】本発明はこのような状況に鑑みてなされたものであり、より変化に富んだ状態で情報を提供することができるようにするものである。

【００１８】

【課題を解決するための手段】請求項１に記載のスクランブルシステムは、パケットを単位として伝送するビデオデータとオーディオデータの少なくとも一方を、パケットを単位としてスクランブルするスクランブル装置において、パケットに含まれるデータが、ビデオデータまたはオーディオデータであることを表すＩＤを検出する検出手段（例えば図３のＩＤ検出部２２Ａ）と、ビデオデータをスクランブルする第１のモード、オーディオデータをスクランブルする第２のモード、ビデオデータとオーディオデータの両方を同時にスクランブルする第３のモード、ビデオデータとオーディオデータを選択的にスクランブルする第４のモードのうちの少なくとも２つのモードの１つを選択的に設定する設定手段（例えば図１の制御回路８３）と、類似ランダム系列を発生する発生手段（例えば図３のＰＲＢＳ生成回路３９と、発生手段の出力する類似ランダム系列をビデオデータまたはオーディオイデータに加算する加算手段（例えば図３の加算器１２）と、設定手段により設定されたモードと、検出手段により検出されたＩＤに対応して、類似ランダム系列の加算手段への供給を制御する制御手段（例えば図３のアンドゲート４）とを備えることを特徴とする。

【００１９】類似ランダム系列を生成するための初期値を、検出手段により検出されたＩＤに対応して修整する修整手段（例えば図３の初期値修整回路２）をさらに備えることができる。

【００２０】同様の構成によりデスクランブルシステムを構成することもできる。

【００２１】請求項５に記載のスクランブル方法は、パケットを単位として伝送するビデオデータとオーディオデータの少なくとも一方を、パケットを単位としてスクランブルするスクランブル方法において、パケットに含まれるデータが、ビデオデータまたはオーディオデータであることを表すＩＤを検出し、ビデオデータをスクランブルする第１のモード、オーディオデータをスクランブルする第２のモード、ビデオデータとオーディオデータの両方を同時にスクランブルする第３のモード、ビデオデータとオーディオデータを選択的にスクランブルする第４のモードのうちの少なくとも２つのモードの１つを選択的に設定し、類似ランダム系列を発生し、発生手段の出力する類似ランダム系列をビデオデータまたはオーディオイデータに加算し、設定されたモードと、検出されたＩＤに対応して、類似ランダム系列の加算手段への供給を制御することを特徴とする。

【００２２】同様の構成によりデスクランブル方法を実現することができる。

【００２３】

【作用】請求項１に記載のスクランブルシステムおよび請求項５に記載のスクランブル方法においては、４つのモードのうち、設定されたモードと、検出されたＩＤに対応して、類似ランダム系列のビデオデータまたはオーディオデータへの加算状態が制御される。したがって、ビデオデータだけあるいはオーディオデータだけをスクランブルしたり、両方を同時にスクランブルしたり、両方を交互にスクランブルしたりすることができ、より変化に富んだ状態を実現することができる。

【００２４】請求項３に記載のデスクランブルシステムおよび請求項６に記載のデスクランブル方法においては、変化に富んだ状態でスクランブルされたデータを確実にデスクランブルすることが可能となる。

【００２５】

【実施例】図１は、上述したＩＳＯ／ＩＥＣ　１３８１８－１（ＭＰＥＧ２　Ｓｙｓｔｅｍｓ）で規定するトランスポートパケットをスクランブルする本発明のスクランブルシステムの構成例を表している。暗号化される前のパケットデータは、スクランブル装置８１に入力され、スクランブルされた後、暗号化されたパケットデータとして出力されるようになされている。入力部８２を操作して、第１のモード乃至第４のモードのうちのいずれか１つのモードを指令すると、制御回路８３は、その指令されたモードに対応する制御信号をスクランブル装置８１に出力する。そして、スクランブル装置８１は、入力された制御信号に対応して、スクランブル動作を行うようになされている。

【００２６】スクランブル装置８１（後述する図３のＩＤ検出部２２Ａ）は、制御回路８３よりビデオデータだけをスクランブルする第１のモードの制御信号が入力された場合、検出したパケットＩＤがビデオパケットであることを表すとき、スクランブルすべきパケットであることを表すＳＣＦ信号をアンドゲート４（図３）に出力する。

【００２７】同様に、オーディオデータだけをスクランブルする第２のモードの制御信号が入力された場合、オーディオデータであることを表すＩＤパケットが検出されたとき、ＳＣＦ信号を出力する。ビデオデータとオーディオデータの両方を同時にスクランブルする第３のモードの制御信号が入力された場合においては、ビデオデ

6

ータのパケットＩＤが検出されたとき、ＳＣＦ信号を出力するだけでなく、オーディオデータのパケットＩＤが検出されたときもＳＣＦ信号を出力する。

【００２８】これに対して、ビデオデータとオーディオデータを選択的にスクランブルする第４のモードの制御信号が入力された場合においては、図２に示すように、任意の数の連続するビデオパケットと、それに隣接する任意の数のオーディオパケットを１つのサイクルとし、第ｉサイクルにおいて、ビデオパケットとオーディオパケットのうち、ビデオパケットを検出したときＳＣＦ信号を出力した場合においては、その次のｉ＋１サイクルにおいては、ビデオパケットを検出したときＳＣＦ信号を出力せず、オーディオパケットを検出したときＳＣＦ信号を出力する。このように、各サイクル毎に交互にビデオパケットまたはオーディオパケットが検出されたときＳＣＦ信号が出力される（スクランブルされる）。

【００２９】図３は、上述したＩＳＯ／ＩＥＣ　１３８１８－１（ＭＰＥＧ２　Ｓｙｓｔｅｍｓ）で規定するトランスポートパケットをスクランブルする図１のスクランブル装置８１の構成例を示すブロック図であり、図７における場合と対応する部分には同一の符号を付してある。すなわちこの実施例においても、初期値レジスタ１乃至加算器１２の構成は、図７における場合と同様である。ただしこの実施例においては、アンドゲート７乃至１０に、修整制御レジスタ５より信号が供給されるとともに、検出回路２２より出力された信号が入力されるようになされている。

【００３０】この検出回路２２は、パケットのヘッダに含まれるパケットＩＤを検出するＩＤ検出部２２Ａと、パケットのヘッダに含まれるｃｏｎｔｉｎｕｉｔｙ－ｃｏｕｎｔｅｒ（継続カウンタ）を検出するＣＣ検出部２２Ｂを有している。

【００３１】その他の構成は図７における場合と同様である。

【００３２】初期値修整回路２は、例えば図４に示すように構成される。この実施例においては、アンドゲート７乃至９より入力される合計１５ビットのデータｇ０乃至ｇ１４が接続マトリックス３１において、３２ビットのデータｈ０乃至ｈ３１に変換され、それぞれ（ｈ０，ｈ１），（ｈ２，ｈ３）・・・（ｈ２８，ｈ２９），（ｈ３０，ｈ３１）のように、２ビットを単位とするデータに区分され、それぞれ加算器３２－１乃至３２－１６に供給される。加算器３２－１乃至３２－１６には、初期値レジスタ１より供給された３２ビットの初期値データｂ０乃至ｂ３１が、（ｂ０，ｂ１），（ｂ２，ｂ３）・・・（ｂ２８，ｂ２９），（ｂ３０，ｂ３１）のように、２ビットずつ区分されて、それぞれ加算器３２－１乃至３２－１６に供給される。

【００３３】加算器３２－１乃至３２－１６は、入力された４ビットのデータからそれぞれ２ビットのデータ（ｃ０，ｃ１），（ｃ２，ｃ３），・・・（ｃ２８，ｃ２９），（ｃ３０，ｃ３１）を生成し、これを修整された初期値としてＰＲＢＳ生成回路３に出力する。

【００３４】ＰＲＢＳ生成回路３は、例えば図５に示すように構成される。この実施例においては、初期値修整回路２の加算器３２－１乃至３２－１６より出力された修整初期値ｃ０乃至ｃ３１のうちｃ０乃至ｃ７が、８段のシフトレジスタで構成されるフィードバックシフトレジスタ４１に入力されている。また、ｃ８乃至ｃ１８が、１１段のシフトレジスタで構成されるフィードバックシフトレジスタ４２に供給されている。さらにｃ１９乃至ｃ３１が１３段のシフトレジスタにより構成されるフィードバックシフトレジスタ４３に供給されている。

【００３５】フィードバックシフトレジスタ４１は、入力ｃ０乃至ｃ７から、データｄ０乃至ｄ７を生成し、このうちｄ０乃至ｄ５を非線形ロジック４４に出力する。フィードバックシフトレジスタ４２は、データｃ８乃至ｃ１８からデータｄ８乃至ｄ１８を生成し、このうちｄ８乃至ｄ１３を非線形ロジック４５に出力する。フィードバックシフトレジスタ４３は、データｃ１９乃至ｃ３１から、データｄ１９乃至ｄ３１を生成し、このうちｄ１９乃至ｄ２４を非線形ロジック４６に供給し、ｄ３１を加算器４８に出力する。

【００３６】非線形ロジック４４は、データｄ０乃至ｄ５から１ビットのデータｐ１を生成し、非線形ロジック４５は、データｄ８乃至ｄ１３からデータｐ２を生成し、非線形ロジック４６は、データｄ１９乃至ｄ２４からデータｐ３を生成する。

【００３７】スイッチ４７は非線形ロジック４５が出力するデータｐ２が０であるとき、図中左側に切り換えられ、非線形ロジック４４の出力ｐ１を選択し、加算器４８に出力する。また、非線形ロジック４５の出力ｐ２が１であるとき、図中右側に切り換えられ、非線形ロジック４６の出力ｐ３を選択し、加算器４８に出力する。加算器４８は、非線形ロジック４４の出力ｐ１または非線形ロジック４６の出力ｐ３と、フィードバックシフトレジスタ４３が出力するデータｄ３１との排他的論理和を演算し、１ビットのＰＮ信号ｐとしてアンドゲート４に出力する。

【００３８】検出回路２２は、入力されるパケットデータからそのヘッダを抽出する。すなわち入力されるパケットデータは、図６に示すようなフォーマットとされている。１パケットの長さは１８８バイトとされ、その先頭の４バイトはヘッダ、残りの１８４バイトがデータ部とされ、そこに実データが配置されるようになされている。

【００３９】ヘッダには、その先頭に８ビットの同期バイトが配置され、続く３ビットを挟んでさらにそれに続く１３ビットはビデオデータ、オーディオデータなどを識別するパケットＩＤ（ＰＩＤ０乃至ＰＩＤ１３）とさ

れている。そして一番最後の４ビットが、ｃｏｎｔｉｎｕｉｔｙ－ｃｏｕｎｔｅｒ（継続カウンタ）の４ビットのデータＣＣＴ０乃至ＣＣＴ３とされている。

【００４０】検出回路２２のＩＤ検出部２２Ａは、図６に示した１３ビットのパケットＩＤＰＩＤ０乃至ＰＩＤ１３を検出し、ＰＩＤ０乃至ＰＩＤ４の５ビットをアンドゲート７に、ＰＩＤ５乃至ＰＩＤ１０の６ビットをアンドゲート８に出力する。そしてＰＩＤ１１乃至ＰＩＤ１３と、ＣＣ検出部２２Ｂにより検出された継続カウンタのデータＣＣＴ０乃至ＣＣＴ３のうちのＣＣＴ０よりなる４ビットがアンドゲート９に出力される。

【００４１】検出回路２２は、パケットヘッダのキー更新タイミングを検出し、キー更新タイミングフラグＳＣＴをアンドゲート６に出力するとともに、制御装置８３から指令されたモードに対応するパケットＩＤを検出したとき、スクランブル識別フラグＳＣＦをアンドゲート４に出力する。

【００４２】また、検出回路２２は、データ部の先頭においてロード信号を出力し、それをアンドゲート１１とＰＲＢＳ生成回路３に出力する。さらに、データ部の先頭以外においては、シフト信号をアンドゲート１１に出力する。

【００４３】次にその動作について説明する。検出回路２２は、データ部の先頭データに加算するＰＮ信号がＰＲＢＳ回路３より出力されるより前の所定のタイミングにおいて、初期値レジスタ１に、１のスクランブルキー更新タイミングフラグＳＣＴを出力し、初期値レジスタ１に、図示せぬ回路から供給される３２ビットの初期値ａ０乃至ａ３１をロードさせる。

【００４４】また、修整制御レジスタ５は、スクランブルキー更新タイミングフラグＳＣＴが１であるとき、図示せぬ回路から供給される４ビットの修整制御値ｅ０乃至ｅ３をロードする。そしてその４ビットのデータをそのまま４ビットの出力ｆ０乃至ｆ３として出力する。

【００４５】すなわち修整制御レジスタ５は、ロード時に次の演算を行う。

【００４６】

【数１】

ロードのとき

$$\sum_{i=0}^{3} f_i x^i \Leftarrow \sum_{i=0}^{1} e_i x^i$$

【００４７】アンドゲート１０は、ＣＣ検出部２２Ｂが検出する継続カウンタの４ビットの値のうち、ＣＣＴ１が１であり、且つ修整制御レジスタ５の出力ｆ３が１であるとき、１のシフト信号を出力する。このシフト信号はキー更新タイミングフラグＳＣＴが０であるとき（先頭以外のとき）、アンドゲート６を通過し、初期値レジスタ１に入力される。初期値レジスタ１はこのシフト信号が入力されると、下位ビットから上位ビットへデータを１ビットづつシフトする。最上位ビットは最下位ビットへシフトされる。初期値レジスタ１を構成する３２段のフィードバックシフトレジスタの生成多項式は、次式で表される。

【００４８】$G1(x) = x^{32} + x^{22} + x^2 + x + 1$

【００４９】入力される初期値ａ０乃至ａ３１に対して、出力をｂ０乃至ｂ３１とするとき、この初期値レジスタ１は、ロード時およびシフト時において次の演算を行うことになる。

【００５０】

【数２】

ロードのとき

$$\sum_{i=0}^{31} b_i x^i \Leftarrow \sum_{i=0}^{31} a_i x^i$$

シフトのとき

$$\sum_{i=0}^{31} b_i x^i \Leftarrow \left(x \times \sum_{i=0}^{31} b_i x^i \right) \bmod G1(x)$$

【００５１】一方アンドゲート７は、ＩＤ検出部２２Ａが検出する１３ビットのパケットＩＤのうち、５ビットのＰＩＤ０乃至ＰＩＤ４と、修整制御レジスタ５の出力ｆ０の論理積を演算し、１５ビットの初期値修整データｇ０乃至ｇ１４のうちの、ｇ１０乃至ｇ１４を生成する。アンドゲート８は、ＩＤ検出部２２Ａが出力するＰＩＤ５乃至ＰＩＤ１０と、修整制御レジスタｆ１との論理積とを演算し、ｇ４乃至ｇ９を生成する。さらにアンドゲート９は、ＩＤ検出部２２Ａが検出するＰＩＤ１１乃至ＰＩＤ１３、およびＣＣ検出部２２Ｂが検出するＣＣＴ０の４ビットのデータと、修整制御レジスタ５の出力ｆ２との論理積を演算し、ｇ０乃至ｇ３を生成する。

【００５２】初期値修整回路２の接続マトリックス３１は、アンドゲート７乃至９より入力される１５ビットの初期値修整データｇ０乃至ｇ１４を、次の表１に示すテーブルにしたがって、データｈ０乃至ｈ３１の３２ビットのデータを生成する。

【００５３】

【表１】

出力	h_0	h_1	h_2	h_3	h_4	h_5	h_6	h_7
入力	g_6	g_0	g_{14}	g_8	g_{10}	g_4	g_2	g_{12}

出力	h_8	h_9	h_{10}	h_{11}	h_{12}	h_{13}	h_{14}	h_{15}
入力	g_8	g_2	g_0	g_{10}	g_{12}	g_6	g_4	g_{14}

出力	h_{16}	h_{17}	h_{18}	h_{19}	h_{20}	h_{21}	h_{22}	h_{23}
入力	g_7	g_1	"0"	g_9	g_{11}	g_5	g_3	g_{13}

出力	h_{24}	h_{25}	h_{26}	h_{27}	h_{28}	h_{29}	h_{30}	h_{31}
入力	g_9	g_3	g_1	g_{11}	g_{13}	g_7	g_5	"0"

【００５４】加算器３２－１乃至３２－１６は、接続マトリックス３１の出力ｈ０乃至ｈ３１と、初期値レジス

タ１の出力ｂ０乃至ｂ３１を、２ビットと単位とする１６のブロックに区分し、次式で示される加算演算を行い、得られた結果をｃ０乃至ｃ３１として、ＰＲＢＳ生成回路３に出力する。

【００５５】

【数３】

$$c_{i+0} = b_{i+0} \oplus h_{i+0}$$

$$c_i = b_i \oplus h_i \oplus (b_{i+0} \cap h_{i+0})$$

$$i = 0, 2, \cdots\cdots, 30$$

ここで、⊕は排他的論理和を、
∩は論理積を表す。

【００５６】ＰＲＢＳ生成回路３は、初期値修整回路２の加算器３２－１乃至３２－１６より出力された３２ビットの修整初期値ｃ０乃至ｃ３１のうち、ｃ０乃至ｃ７をフィードバックシフトレジスタ４１に、ｃ８乃至ｃ１８をフィードバックシフトレジスタ４２に、そしてｃ１９乃至ｃ３１をフィードバックシフトレジスタ４３に、それぞれロードする。

【００５７】フィードバックシフトレジスタ４１は、８段のシフトレジスタで構成され、次式で表される生成多項式Ｇ２（ｘ）に従い、入力ｃ０乃至ｃ７に対して、データｄ０乃至ｄ７を生成する。

【００５８】Ｇ２（ｘ）＝$x^8+x^4+x^3+x^2+1$

【００５９】フィードバックレジスタ４２は、１１段のシフトレジスタにより構成され、次式で表される生成多項式Ｇ３（ｘ）を用いて、入力ｃ８乃至ｃ１８に対してデータｄ８乃至ｄ１８生成する。

【００６０】Ｇ３（ｘ）＝$x^{11}+x^2+1$

【００６１】フィードバックシフトレジスタ４３は、１３段のシフトレジスタで構成され、次式で表される生成多項式Ｇ４（ｘ）を用いて、入力ｃ１９乃至ｃ３１に対して、データｄ１９乃至ｄ３１を生成する。

【００６２】Ｇ４（ｘ）＝$x^{13}+x^4+x^3+x+1$

【００６３】データのシフトは各パケットのデータに対応するクロックを用いて、下位ビットから上位ビットに向けて行われる。

【００６４】以上のフィードバックシフトレジスタ４１乃至４３におけるロードと、シフトの動作をまとめると次の式で表すことができる。

【００６５】

【数４】

ロードのとき

$$\sum_{i=0}^{31} d_i x^i \Leftarrow \sum_{i=0}^{31} c_i x^i$$

シフトのとき

$$\sum_{i=0}^{31} d_i x^i \Leftarrow \{(x \times \sum_{i=0}^{7} d_i x^i) \bmod G2(x)\} \div \{(x \times \sum_{i=8}^{18} d_i x^i) \bmod (x^8 \times G3(x))\} \div \{(x \times \sum_{i=19}^{31} d_i x^i) \bmod (x^{19} \times G4(x))\}$$

【００６６】非線形ロジック４４には、フィードバックシフトレジスタ４１が生成したデータｄ０乃至ｄ７のうち、６ビットのデータｄ０乃至ｄ５が入力される。非線形ロジック４４は、このデータｄ０乃至ｄ５を入力とし、１ビットのデータｐ１を生成する。

【００６７】同様に非線形ロジック４５には、フィードバックシフトレジスタ４２が生成するデータｄ８乃至ｄ１７のうち、ｄ８乃至ｂ１３が入力され、非線形ロジック４５は、このデータｄ８乃至ｄ１３から、１ビットのデータｐ２を生成する。

【００６８】また、非線形ロジック４６には、フィードバックシフトレジスタ４３が生成するデータｄ１９乃至ｄ３１のうち、ｄ１９乃至ｄ２４が入力され、非線形ロジック４６は、このデータｄ１９乃至ｄ２４から１ビットのデータｐ３を生成する。

【００６９】ｉ＝０，８，１９における６ビットの入力（d_{i+5}，d_{i+4}，d_{i+3}，d_{i+2}，d_{i+1}，d_i）の（０，０，０，０，０，０），（０，０，０，０，０，１），（０，０，０，０，１，０），・・・，（１，１，１，１，１，１）に対応する１ビットの出力ｐをそれぞれ、（ｐ（０，０，０，０，０，０），（ｐ（０，０，０，０，０，１），・・・，ｐ（０，１，１，１，１，１），（ｐ（１，０，０，０，０，０），（ｐ（１，０，０，０，０，１），・・・，ｐ（１，１，１，１，１，１））で表すものとすると、非線形ロジック４４乃至４６の出力は、次のように表すことができるようにす

る。

【００７０】非線形ロジック４４

（0，0，0，0，1，1，1，0，0，1，1，1，
0，0，1，1，0，0，1，1，0，1，0，0，
1，0，0，1，0，1，1，0，1，1，1，1，
0，0，0，1，0，1，1，0，1，0，0，0，
1，0，0，0，1，0，1，1，0，0，1，1，
1，1，0，1）

【００７１】非線形ロジック４５

（0，1，1，0，0，1，1，0，1，0，0，1，
1，0，1，1，0，1，1，0，1，0，0，1，
0，0，1，1，0，1，0，0，0，0，0，1，
1，1，1，1，1，0，0，0，0，1，1，1，
1，1，1，0，0，0，1，1，0，1，0，1，
0，0，0，0）

【００７２】非線形ロジック４６

（1，0，1，0，1，1，0，1，0，1，1，0，
0，0，0，1，1，1，0，1，0，0，0，0，
1，0，1，1，1，0，1，1，0，1，0，1，
0，0，1，1，1，0，1，1，1，1，1，0，
0，1，1，0，1，0，0，1，0，0，0，0，
0，0，0，1）

【００７３】そして、非線形ロジック４５の出力ｐ２が０であるとき、スイッチ４７は、非線形ロジック４４の出力ｐ１を選択し、加算器４８に出力する。また非線形ロジック４５の出力ｐ２が１であるとき、スイッチ４７は非線形ロジック４６の出力ｐ３を加算器４８に出力する。

【００７４】加算器４８は、非線形ロジック４４の出力ｐ１、または非線形ロジック４６の出力ｐ３と、フィードバックシフトレジスタ４３の出力ｄ３１との排他的論理和の演算を行い、１ビットのＰＮ信号ｐを生成する。

【００７５】すなわち、スイッチ４７と、加算器４８により、次の演算が行われることになる。

【００７６】

【数５】

$$p = \{(p1 \cap \overline{p2}) \cup (p3 \cap p2)\} \oplus d31$$

ここで、$\overline{\ }$は否定、∩は論理積、∪は論理和、⊕は排他的論理和を表す。

【００７７】ＰＲＢＳ生成回路３が出力するデータｐは、スクランブル識別フラグＳＣＦが１であるとき（スクランブルすべきパケットであるとき）、アンドゲート４を介して、加算器１２に供給され、パケットデータとの排他的論理和が演算されて、暗号化されたパケットデータとして出力される。

【００７８】そして、検出回路２２は、制御装置８３を介して入力部８２より入力されるモードに対応してＳＣＦ信号をアンドゲート４に出力する。その結果、第１のモードにおいてはビデオパケットだけが、第２のモードにおいてはオーディオパケットだけが、第３のモードにおいてはビデオパケットとオーディオパケットの両方が、第４のモードにおいてはビデオパケットとオーディオパケットが交互に、それぞれスクランブルされる。

【００７９】なお、上記実施例においては、ＰＩＤ０乃至ＰＩＤ１３、およびＣＣＴ０、ＣＣＴ１から初期値補正データを生成するようにしたが、この他、ＣＣＴ２、ＣＣＴ３を用いるようにすることもできる。

【００８０】なお、データ部に記録される実データとしては、映像データ、音声データ、その他のデータの他、任意のデータとすることができる。

【００８１】また上記実施例においては、スクランブル装置を説明したが、全く同様の構成により、デスクランブル装置を実現することができる。

【００８２】

【発明の効果】以上の如く、請求項１に記載のスクランブルシステムおよび請求項５に記載のスクランブル方法によれば、第１のモード乃至第４のモードのうち、設定されたモードと検出されたＩＤに対応して、類似ランダム系列のビデオデータまたはオーディオデータへの加算を制御するようにしたので、より変化に富んだ状態で、ビデオデータまたはオーディオデータをスクランブルすることができる。

【００８３】その結果、例えば音楽を中心とする番組においては、主要な情報であるオーディオデータはスクランブルするが、ビデオデータはスクランブルしないようにして、あえて画像をモニタさせることで、それに付随するオーディオを聞きたくなるようにさせたり、その逆に、例えば映画などのように、様々な画面における画像が中心となる番組においては、ビデオデータをスクランブルし、オーディオデータをスクランブルしないようにして、オーディオだけをモニタさせて、その番組に興味を持たせるようにすることができる。あるいはまた、局部的に（極めて短時間だけ）画像をモニタさせたり、音声をモニタさせることにより、その番組に興味を持たせるなどすることができる。

【００８４】また、請求項３に記載のデスクランブルシステムおよび請求項６に記載のデスクランブル方法によれば、上述したスクランブルシステムおよび方法における場合と同様の効果を奏することができる。

【図面の簡単な説明】

【図１】本発明のスクランブルシステムの構成例を示すブロック図である。

【図２】ビデオパケットとオーディオパケットを交互にスクランブルする例を示す図である。

【図３】図１のスクランブル装置８１の構成例を示すブロック図である。

【図４】図３の初期値修整回路２の構成例を示すブロック図である。

【図５】図３のＰＲＢＳ生成回路３の構成例を示すブロ

ック図である。

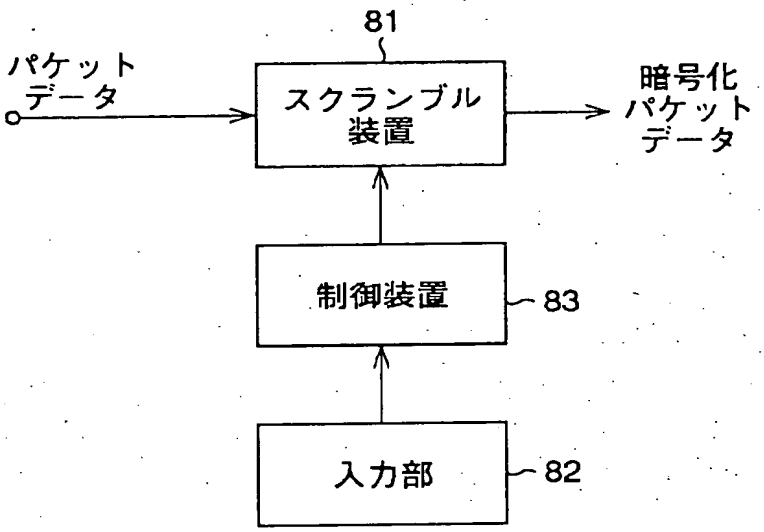
【図６】トランスポートパケットのフォーマットを説明する図である。

【図７】従来のスクランブル装置の構成例を示すブロック図である。

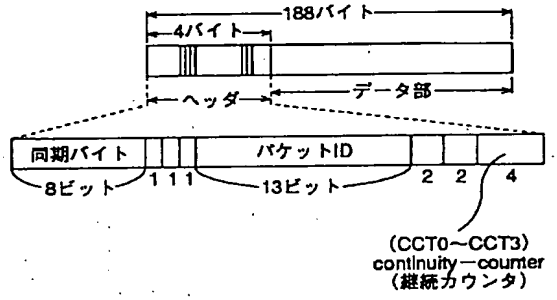
【符号の説明】

１　初期値レジスタ
２　初期値修整回路
３　ＰＲＢＳ生成回路
５　修整制御レジスタ
２１　キー切り換え回路
２２　検出回路
２２Ａ　ＩＤ検出部
２２Ｂ　ＣＣ検出部
３１　接続マトリックス
３２－１乃至３２－１６　加算器
４１乃至４３　フィードバックシフトレジスタ
４４乃至４６　非線形ロジック
４７　スイッチ
４８　加算器
６１，６２　キーレジスタ
６３　セレクタ

【図１】

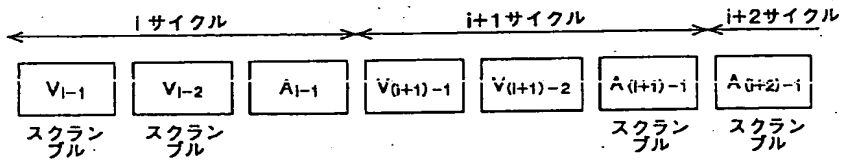


【図６】

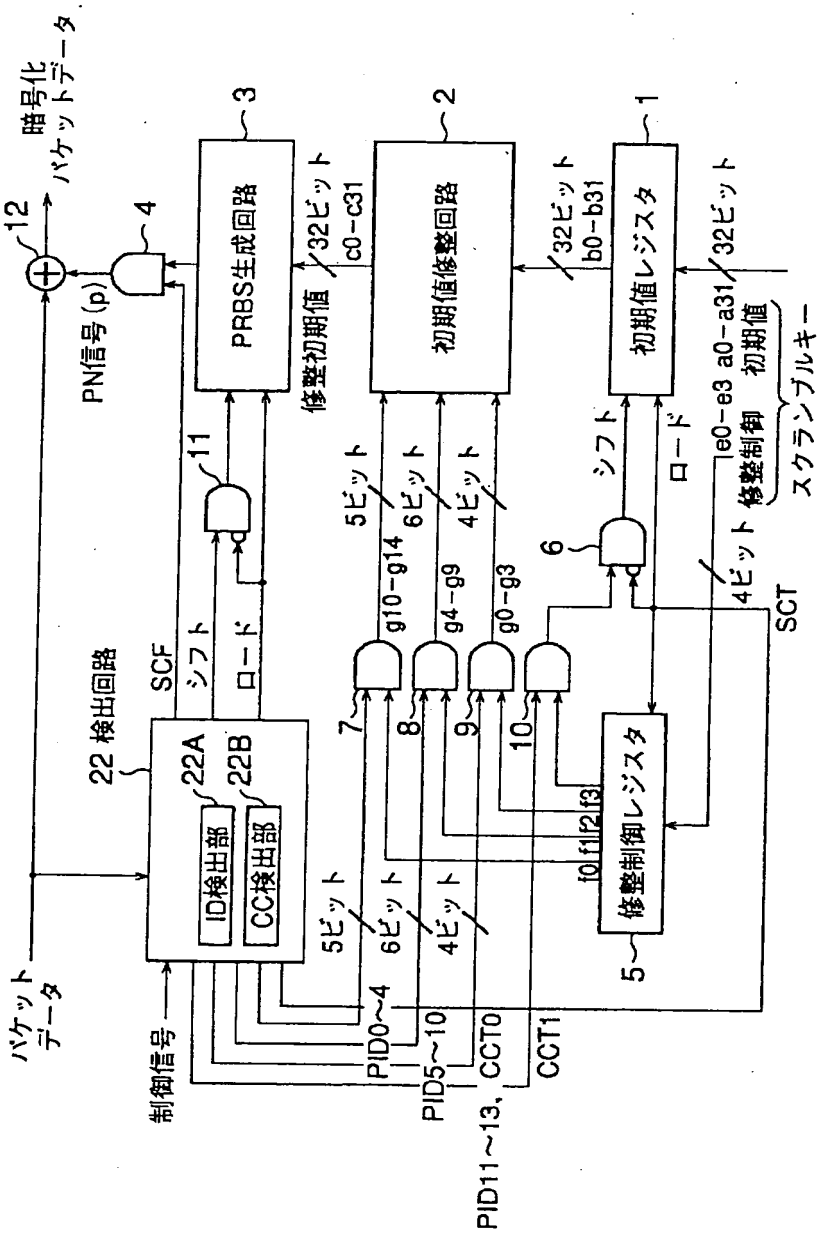


トランスポートパケット

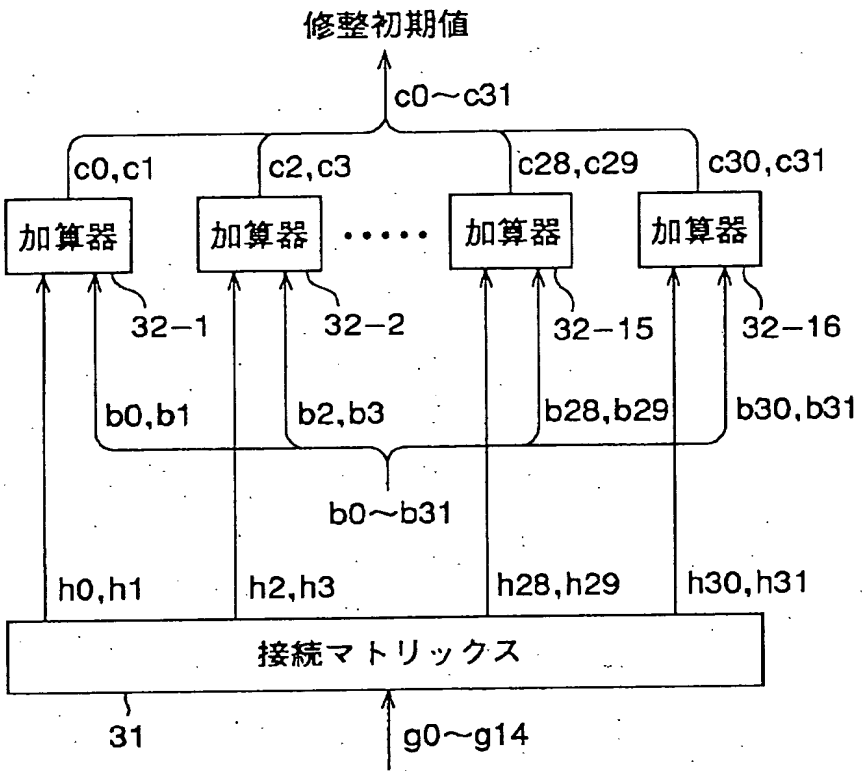
【図２】



【図３】

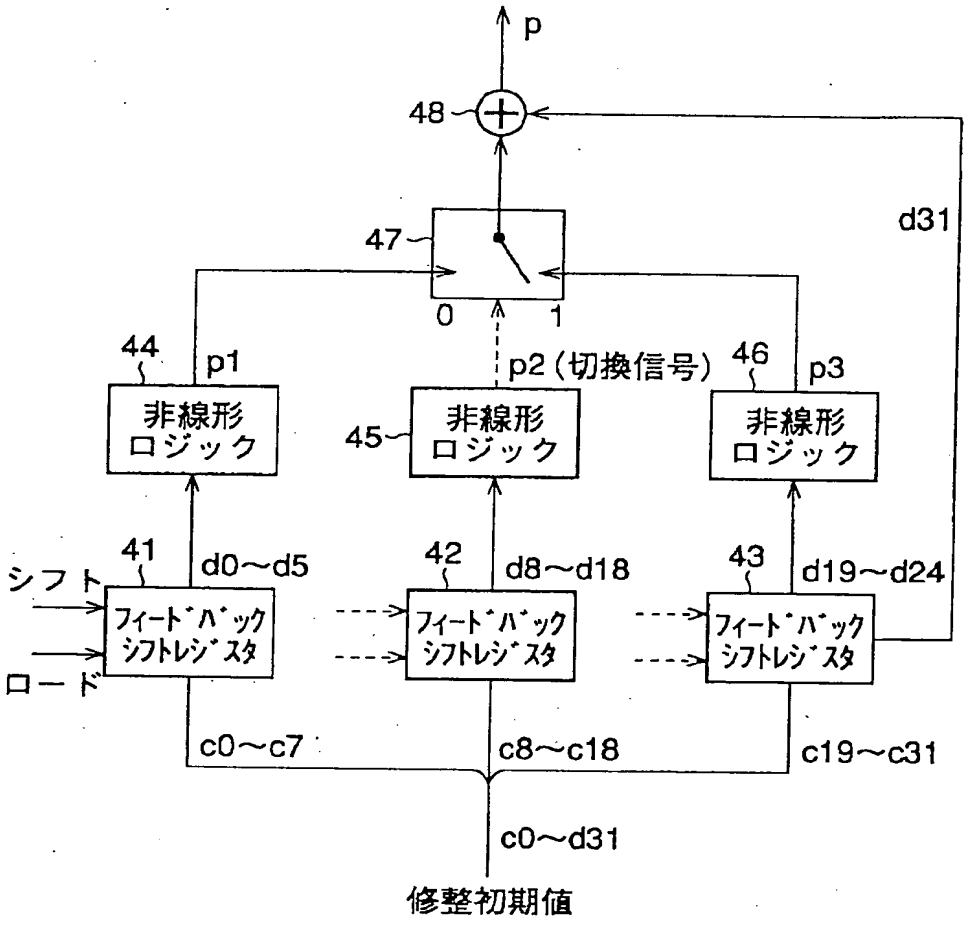

暗号化
パケットデータ
12
PN信号(p)
4
PRBS生成回路
3
修整初期値
32ビット
c0-c31
初期値修整回路
2
32ビット
b0-b31
初期値レジスタ
1
32ビット
e0-e3 a0-a31
初期値
修整制御
スクランブルキー
11
SCF
シフト
ロード
22 検出回路
22A
ID検出部
22B
CC検出部
5ビット
6ビット
4ビット
g10-g14
g4-g9
g0-g3
7
8
9
10
6
シフト
ロード
4ビット
SCT
f0 f1 f2 f3
修整制御レジスタ
5
パケットデータ
制御信号
PID0~4
PID5~10
PID11~13,
CCT0
CCT1

【図４】


修整初期値
c0～c31
c0,c1
c2,c3
c28,c29
c30,c31
加算器
加算器
・・・・・
加算器
加算器
32－1
32－2
32－15
32－16
b0,b1
b2,b3
b28,b29
b30,b31
b0～b31
h0,h1
h2,h3
h28,h29
h30,h31
接続マトリックス
31
g0～g14

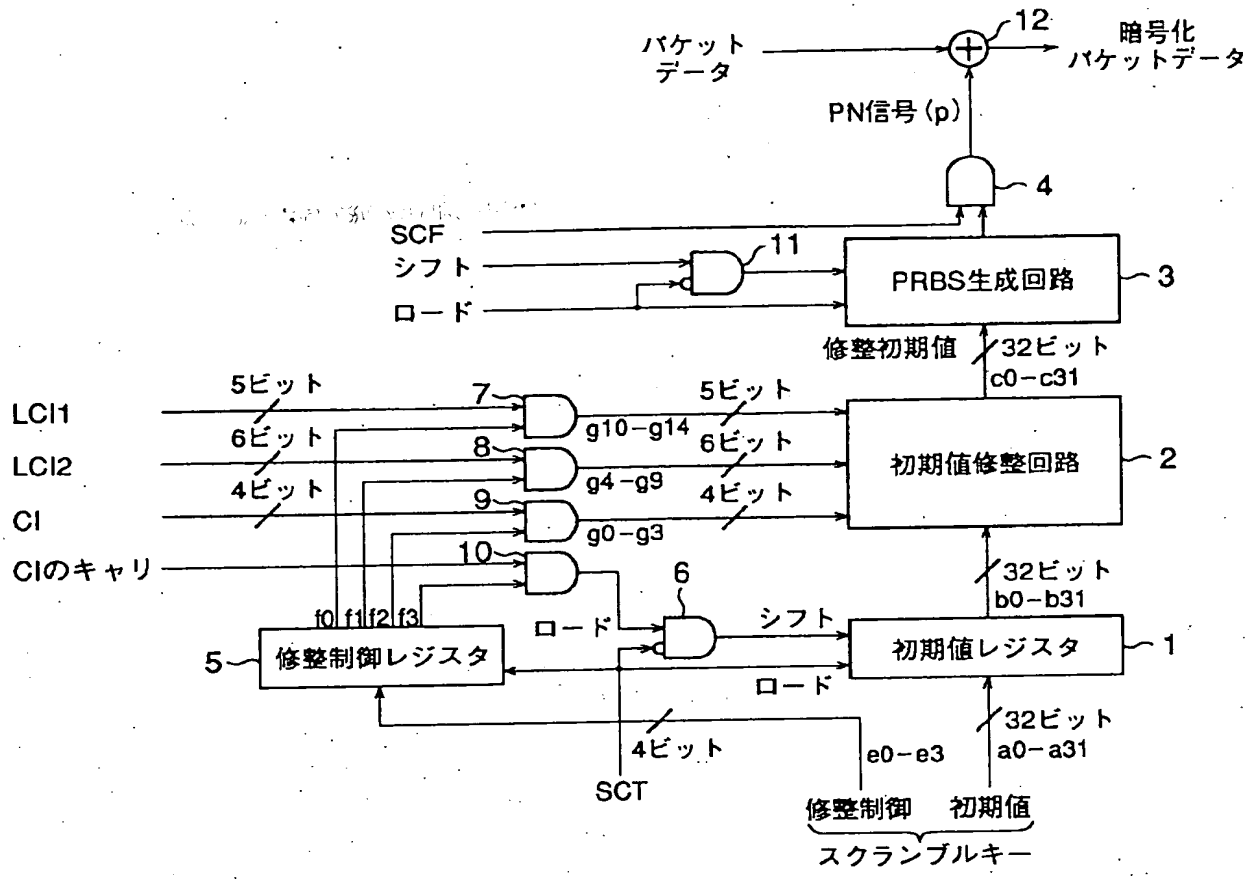
初期値修整回路２

【図５】



PRBS生成回路３

【図７】



フロントページの続き

(51)Int.Cl.'	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　9/18				
Ｈ０４Ｎ　7/167				